



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

Address: COMMISSIONER FOR PATENTS

P.O. Box 1450

Alexandria, Virginia 22313-1450

www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/611,402	06/30/2003	Winifred Washington	013628.00499 (02CXT0078D)	1911
77339 7590 02/03/2010 JACKSON WALKER (CONEXANT) 901 MAIN STREET, SUITE 6000 DALLAS, TX 75202				
EXAMINER				
JACKSON, JENISE E				
ART UNIT		PAPER NUMBER		
2439				
MAIL DATE		DELIVERY MODE		
02/03/2010		PAPER		

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/611,402

Applicant(s)

WASHINGTON, WINEFRED

Examiner

JENISE E. JACKSON

Art Unit

2439

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 05 January 2010.
2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-5, 7-15 and 17-28 is/are pending in the application.
4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5) ☐ Claim(s) _____ is/are allowed.
6) ☒ Claim(s) 1-5, 7-15, 17-28 is/are rejected.
7) ☐ Claim(s) _____ is/are objected to.
8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB-08)
4) ☐ Interview Summary (PTO-413)
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____
Paper No(s)/Mail Date _____

DETAILED ACTION

Claim Rejections - 35 USC § 112

1. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claim 1 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.
3. Claim 1 claims, “wherein the integrated encryption key generator is coupled between the data buffer”. Claim 1, fails to particularly point out and distinctly claim the subject matter which the application regards as the invention, because the claim 1, is missing elements. An example, on page 4, discloses the encryption circuit is placed between the data buffer and the I/O register. Claim 1 only claims the integrated encryption key generator is coupled between the data buffer. Correction is required.

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2. Claim 1-5, 7-15, 17-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Halpern(2006/0239453) in view of Lyle(2008/0046728).

3. As per claim 1, Halpern discloses a data buffer [0063]; an input/output register that interfaces with memory of the digital device [0050], and a memory controller that directs digital data from the memory to the data buffer with the digital data passing thorough the encryption key generator prior to entering the input/output register[0063], wherein the data buffer, input/output register and the memory controller are contained within an enclosed digital device[0050, 0063]. Halpern discloses the encryption key generator is coupled to a data buffer[0063].

4. Halpern is silent on an integrated encryption key generator generating at least one key based on input received from an inaccurate timing source, Halpern is silent on the integrated encryption key generator is enclosed within the digital device. Lyle discloses integrated encryption key generator generating at least one key based on input received from an inaccurate (i.e. R-C oscillator affected by temperature, voltage, noise or other physical forces)[0132] timing source(i.e. R-C oscillator), and Lyle discloses the integrated encryption key generator is enclosed within the digital device(i.e. transmitter)[0020, 0055].

5. It would have been obvious to one of ordinary skill in the art at the time of the invention to include an integrated encryption key generator generating at least one key based on input received from an inaccurate timing source of Lyle with Halpern, the motivation is that generating at least one key based on input received from an inaccurate timing source insures that a key that is generated by using this method is difficult or impossible for an attacker to place the transmitter in the same initial state, because the key is based on an inaccurate clock, that can be inaccurate due to temperature or voltage or noise, or other physical forces[0132 of Lyle].

6. Same Motivation as above. As per claim 2, Halpern discloses a key store[0045] and a linear feedback shift register[0014] generates a pseudorandom bit pattern while the linear feedback shift register is enabled and stores a plurality of bits as at least one key in the key store[0014, 0063]. Halpern is silent on an inaccurate clock. Lyle discloses an inaccurate clock[0132].
7. As per claim 3, Halpern discloses where the encryption key generator further includes a random number generator that receives the pseudorandom bit pattern from the linear feedback shift register and provides a random number for use by the digital device[0039, 0050].
8. As per claim 4, Halpern discloses pseudorandom bit pattern that creates a bit stream; and a key store that stores portions of pseudorandom bit pattern as the at least one keys[0050, 0063].
9. As per claim 5, Halpern discloses including a pseudo random number generator that selects a portion of the pseudorandom bit pattern to be random number[0052].
10. As per claim 7, Halpern discloses a subkey that creates a sub-key based on data from the memory controller and a selected key from the key store; and a combiner that combines the sub-key with the digital data[0069].
11. As per claim 8, Halpern discloses a data mixer that mixes the bits of a byte of digital data; and a combiner that combines the byte of the digital data prior to the byte being combined with the sub-key[0062, 0069].
12. Same Motivation as claim 1. As per claims 9, 22, Halpern discloses a memory controller that generates a memory request to retrieve the encrypted digital data; and encryption circuit that decrypts the encrypted digital data in response to the memory request of the memory controller using one key[0045-0046]. Halpern is silent on decrypt encrypted digital data stored in memory

of a digital device, an encryption key generator receiving a signal from an inaccurate clock and generating a plurality of keys for encrypting the encrypted digital data. Lyle discloses decrypt encrypted digital data stored in memory of a digital device, and encryption key generator receiving a signal from an inaccurate clock and generating a plurality of keys for encrypting the encrypted digital data[0055, 0022, 0026, 0132].

13. As per claim 10, Halpern discloses a combiner that combines one of the plurality of keys with a bank and row information contained in the memory request resulting in a sub-key[0062, 0069].

14. As per claim 11, Halpern discloses a data mixer that unmixes bits within a byte after the sub-key is applied to encrypted digital data[0062, 0069].

15. As per claim 12, Halpern discloses generating at least one key, placing the digital data in a data buffer; and encrypting the digital data using the at least one key while the digital data is being placed[0022, 0045, 0063].

16. Same Motivation as claim 1. As per claim 13, Halpern discloses creating a pseudorandom bit pattern, and storing at least one portion of the pseudorandom bit pattern in a key store as the at least one key[0052]. Halpern is silent on disclosing generating of an inaccurate clock. Lyle discloses generating a key based on an inaccurate clock signal[0132].

17. As per claim 14, Halpern discloses where the pseudorandom bit pattern is generated by a linear feedback shift register[0064].

18. As per claims 15, 21, Halpern discloses generating a random number from the pseudorandom bit pattern[0039, 0050].

19. As per claim 17, Halpern discloses selecting a portion of the pseudorandom bit pattern to be used a random number[0050].
20. As per claim 18, Halpern discloses mixing the bits of a byte of the digital data with a data and combining the byte with the at least one key[0062, 0069].
21. As per claim 19, Halpern discloses generating a sub-key with data from the memory controller and the key; and combining the sub-key with the digital data[0069].
22. As per claim 20, Halpern discloses mixing the bits of byte of digital data with a data mixer; and combining the byte with the sub-key[0050].
23. As per claim 23, Halpern discloses combining the at least one key with a bank and row information contained in the memory request to generate a sub-key[0062, 0069].
24. As per claim 24, Halpern discloses unmixing a byte of encrypted digital data with a data mixer[0069].
25. As per claim 25, Halpern discloses an encryption circuit with at least one key, a data buffer filled with the digital data[0022, 0045, 0063], a memory controller that directs and the storage of digital data in the rewriteable memory with the digital data being encrypted by the encryption circuit and the at least one key after the digital data has entered the data buffer but prior to being stored in the rewritable memory[0063].
26. As per claim 26, Halpern discloses a pseudorandom bit stream generator that creates a pseudorandom bit stream; and a key store that stores the at least one key that is selected from the pseudorandom bit stream[0052].
27. As per claims 27, Halpern discloses a data mixer mixes the bits of a byte of the digital data; and a combiner that combines the byte with the key[0050].

28. As per claims 28, Halpern discloses wherein the memory controller that directs digital data from the memory to the data buffer with the digital data passing through the encryption key generator prior to entering the input/output register comprises means for encrypting the digital data prior to entering the input/output register[0063].

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JENISE E. JACKSON whose telephone number is (571)272-3791. The examiner can normally be reached on Increased Flex time, but generally in the office M-Fri(8-4:30)..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Edan Orgad can be reached on (571) 272-7884. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Application/Control Number: 10/611,402

Page 8

Art Unit: 2439

/J. E. J./

Examiner, Art Unit 2439

/Edan Orgad/

Supervisory Patent Examiner, Art Unit 2439